COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, CHAIRMAN

NEWS RELEASE

For Immediate Release
September 27, 2006

Contact: David Marin/Brian McNicoll
(202) 225-5074

Davis Data Breach Bill Approved by House

WASHINGTON, D.C. – Legislation introduced by Rep. Tom Davis (R-Va.) to require federal agencies to better protect the sensitive information in their care was approved by the House Tuesday as part of a Veterans Administration bill to protect sensitive data.

The bill now moves to the Senate. If it passes there, it would move to the White House for the president's signature. If the Senate does not act, Davis has said he will try to move his language separately in November.

Davis' legislation would require all federal agencies to tell the public when data breaches involving sensitive information occur. This language amends the Federal Information Security Management Act, which Davis introduced and shepherded to passage in 2002.

Davis' legislation directs the Office of Management and Budget to establish procedures for agencies to follow if personal information is lost or stolen. It also would require that individuals be notified if their personal information could be compromised by a breach of data security at a federal agency. It would give Chief Information Officers the power to ensure, when authorized by an agency head, that agency personnel comply with information security laws. The bill also requires agencies to ensure that costly equipment containing sensitive information is accounted for and secure.

As originally drafted, the Davis language (HR 5838) became part of the VA bill, which was introduced after officials there revealed a laptop computer containing sensitive information about veterans had been stolen from an employee's home in suburban Maryland. Davis added the revised legislation (HR 6163) to the VA bill yesterday.

After the VA incident, the Committee on Government Reform, which Davis chairs, asked other federal agencies if they were missing laptops or other potentially compromising information. The Commerce Department revealed it couldn't account for more than 1,100 laptops, some containing census data. Half the missing computers were simply not returned by departing or terminated employees. Some agencies have yet to respond to the committee's query.

"This bill is a first step," said Davis. "If new policies and procedures are not forthcoming quickly, or if they lack the teeth to get the job done, I will revisit this matter with additional legislation."

###

Here is Rep. Davis' floor statement from Wednesday night, in support of his data breach legislation:

Federal Agency Data Breach Protection
Chairman Tom Davis
September 26, 2006
Consideration of HR 5835 (Veterans Identity and Credit Security Act of 2006)

Secure information is the lifeblood of effective government policy and management, yet federal agencies continue to hemorrhage vital data. Recent losses of personal information compel us to ask: What is being done to protect the sensitive digital identities of millions of Americans, and how can we limit the damage when personal data does go astray?

As we all now know, a Department of Veterans Affairs employee reported the theft of computer equipment from his home, equipment that stored more than 26 million records containing personal information.

VA leadership delayed acting on the report for almost two weeks, while millions were at risk of serious harm from identity theft and the agency struggled to determine the exact extent of the breach.

But this is only one in a long string of personal information breaches in the public and private sectors, including financial institutions, data brokerage companies, and academic institutions. Just last week we learned that the Census Bureau cannot account for 1,100 laptops issued to employees.

These breaches illustrate how far we have to go to reach the goal of strong, uniform, government-wide information security policies and procedures.

On the Government Reform Committee, we've been focused on government-wide information management and security for a long time. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. These recent incidents highlight the importance of establishing – and following -- security standards for safeguarding personal information. They also highlight the need for pro-active security breach notification requirements for organizations -- including federal agencies -- that deal with sensitive personal information.

Congress has been working on requirements for the private sector. But Federal agencies present unique requirements and challenges, and these incidents demonstrate that we need to strengthen the laws and rules protecting personal information held by federal agencies.

Given the VA incident, and in order to get a more complete picture of the problem before pursuing legislation, my Committee sent a request to all cabinet agencies seeking information about data breaches involving the loss of sensitive personal information.

The results are in and they are troubling. We've learned that there have been a wide range of incidents involving data loss or theft, privacy breaches, and security incidents.

In almost all of these cases, Congress and the public would not have learned each event unless we had requested the information. This history of withholding incidents has to stop.

My bill (HR 6163) – which has been incorporated as a manager's amendment in Section 2 of the bill before us -- requires that timely notice be provided to individuals whose sensitive personal information could be compromised by a breach of data security at a federal agency. Despite the volume of sensitive information held by agencies, until now, there has been no requirement that people be notified if their information is compromised. Under this legislation, the Administration must establish practices, procedures and standards for agencies to follow if sensitive personal information is lost or stolen and there is a reasonable risk of harm to an individual. And we provide a clear definition of the type of sensitive information we're trying to protect.

We also give the agency Chief Information Officers the authority, when appropriate and authorized, to ensure that agency personnel comply with the information security laws already on the books.

Finally, we ensure that costly equipment containing potentially sensitive information is accounted for and secure. Half of the lost Census Bureau computers simply were not returned by departing or terminated employees. The agency did not track computer equipment, nor were employees held accountable for failing to return it. This is taxpayer funded equipment, containing sensitive information, and we must know what we have and who has it at all times.

Each year, my Committee releases information security scorecards. This year the scores for many departments remained unacceptably low or dropped precipitously. The Veterans Affairs Department earned an F, the second consecutive year and fourth time in the past five years the department receiving a failing grade. The federal government overall received a D+.

The federal government has sensitive personal information on every citizen – health records, tax returns, military records. If the federal government can't secure this information, who can? We need to ensure the public knows when its sensitive personal information has been lost or compromised in some way.

I want to commend my colleagues who have worked with me on the data breach issues. Chairman Buyer, Ms. Pryce, and Mr. Sweeney all recognize the importance of securing personal information held by federal agencies, and I appreciate their work and support on this issue.

The provisions we included in this bill are a first step. If new policies and procedures are not forthcoming quickly, or if they lack the teeth to get the job done, I will revisit this matter with additional legislation.